IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (**Currently Amended**) A method performed by a user terminal of a wireless access network, the method comprising:

generating a shared secret to be provided to an access point of the wireless access network;

encrypting the shared secret with an access point public key;

pre-calculating a plurality of authenticator messages based on a corresponding plurality of estimated time parameters, each authenticator message comprising at least part of the shared secret;

receiving an indication of ~~an actual~~ **a measured** time parameter; and

selecting a pre-calculated authenticator message that corresponds to the ~~actual~~ **measured** time parameter; and

signing the selected authenticator message with a user terminal private key; and

sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate, and the signed authenticator message.

2. (Original) The method of claim 1, wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

3. (Original) The method of claim 2, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point.

4. (Cancelled)

5. (Previously Presented) The method of claim 1, wherein signing the authenticator message comprises:

generating a digest of the authenticator message; and

encrypting the authenticator message digest with the user terminal private key.

6-7. (Cancelled)

8. (**Currently Amended**) The method of claim 1, wherein the **estimated** time parameter**s comprise absolute frame numbers and the measured time parameter** comprises an absolute frame number.

9. (Previously Presented) The method of claim 1, wherein the user terminal generates and encrypts the shared secret prior to identifying the access point by encrypting the shared secret with the public keys of a plurality of access points stored in the user terminal.

10-16. (Cancelled)

17. (**Currently Amended**) A user terminal comprising:

a memory to store a user terminal certificate and a shared secret to be provided to an access point;

a processor coupled to the memory to

encrypt the shared secret with access point public key,

pre-calculate a plurality of authenticator messages based on a corresponding plurality of estimated time parameters, each authenticator message comprising at least part of the shared secret;

receive an indication of ~~an actual~~ **a measured** time parameter,

select a pre-calculated authenticator message that corresponds to the ~~actual~~ **measure** time parameter, and

sign the selected authenticator message with a user terminal private key; and

a transmitter coupled to the processor to send a message to the access point, the message including the encrypted shared secret, the user terminal certificate, and the signed authenticator message.

18. (Original) The user terminal of claim 17, wherein the processor is further to scramble the user terminal certificate using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

19. (Original) The user terminal of claim 18, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point.

20. (Cancelled).

21. (Previously Presented) The user terminal of claim 17, wherein signing the authenticator message comprises:

generating a digest of the authenticator message; and

encrypting the authenticator message digest with the user terminal private key.

22-23. (Cancelled)

24. (**Currently Amended**) The user terminal of claim 17, wherein the **estimated** time parameter**s comprise absolute frame numbers and the measured time parameter** comprises an absolute frame number.

25-32. (Cancelled)

33. (**Currently Amended**) A machine-readable medium storing data representing instructions that, when executed by a processor of a user terminal, cause the processor to perform operations comprising:

generating a shared secret to be provided to an access point of the wireless access network;

encrypting the shared secret with an access point public key;

pre-calculating a plurality of authenticator messages based on a corresponding plurality of estimated time parameters, each authenticator message comprising at least part of the shared secret;

receiving an indication of ~~an actual~~ **a measured** time parameter; and

selecting a pre-calculated authenticator message that corresponds to the ~~actual~~ **measured** time parameter; and

signing the selected authenticator message with a user terminal private key; and

sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate, and the signed authenticator message.

34. (Original) The machine-readable medium of claim 33, wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

35. (Original) The machine-readable medium of claim 34, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point.

36. (Cancelled).

37. (**Currently Amended**) The machine-readable medium of claim **33** ~~36~~, wherein signing the authenticator message comprises:

generating a digest of the authenticator message; and

encrypting the authenticator message digest with the user terminal private key.

38-39. (Cancelled)

40. (**Currently Amended**) The machine-readable medium of claim **33** ~~39~~, wherein the **estimated** time parameter**s comprise absolute frame numbers and the measure time parameter** comprises an absolute frame number.

41-49. (Cancelled)